



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/840,230	04/24/2001	Stuart Gerald Stubblebine	2455-4230US3	5050

7590 06/17/2004

Mr. S H Dworetsky  
AT&T Corp  
P O Box 4110  
Middletown, NJ 07748

EXAMINER

AKPATI, ODAICHE T

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 06/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/840,230

Applicant(s)

STUBBLEBINE, STUART GERALD

Examiner

Tracey Akpati

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 29 March 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 52-56 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 52-56 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 24 April 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

1. Claims 52-56 have been submitted. Claims 53 and 54 have been amended. The attorney's amendment has necessitated change in the grounds of rejection. This action is final.

#### ***Response to Arguments***

2. With respect to Claim 56, Abadi on pages 204-205, section 2.3 does not disclose a 'language tutorial' as the attorney might suggest. Abadi discloses the heart of the applicant's invention which are the assertion of freshness constraints. Abadi discloses that the freshness of a message is proven by including a nonce such as a timestamp within the message being sent to verify its freshness. This occurs over a network such as the one shown in Abadi, Figure 1 on page 201. A server S, and two stations A and B are shown as part of a network. The timestamp Ts allows A to believe that S sent the message recently.

The server S represents the revocation authority because it generates a message containing a timestamp, Ts to prove to the recipient A that the message has been sent recently (see pg. 201, column 2) or are fresh meaning that they have not been sent before the start of the current authentication (see page 202, column 1).

3. With respect to Claim 56, the first and second limitation is met by Figure 1. The message sent by the server on channel 2 includes a timestamp based on its freshness policy. The revocation authority is the server S. The verification authority step is inherently disclosed on pg. 201 at station A and B. If A can decrypt a message sent by S with a key  $K_{AS}$  known only to A and S, then A believes the message must have come from S and hence authenticates/verifies S. A also

believes from the recent timestamp  $T_s$  that S sent the message recently. The same reasoning applies to station B. Hence the verification steps substitutes for a verification authority because stations A and B perform the verification process that would have been done by a verification authority.

4. With respect to Claim 52-54, the attorney argues that column 2, page 201 does not teach “deriving freshness constraints from initial policy assumptions and an authentic statement.”

Figure 1 on page 201 of Abadi clearly shows freshness constraints of a timestamp contained with an authentic statement shown within the message sent from the server to station A. The initial policy assumptions are that if the message contains a recent timestamp  $T_s$ , A believes that S sent the message recently. Contrary to what the attorney might think, time has everything to do with freshness. (see Abadi, page 202, column 1). It says timestamps are used to prove that messages are fresh. This is a direct admission that time is directly related to the freshness of a message, contrary the attorney’s statement.

5. The attorney further argues that  $|t_{\text{now}} - t_{\text{timestamp}}| \leq \delta$  is not the same thing as  $|\text{Clock} - T| \leq \Delta t_1 + \Delta t_2$  with respect to the right hand side of these inequalities.

(See Denning, page 534, column 2)  $\Delta t_1$  is an interval between the server’s clock and the local clock  $\Delta t_2$  is an interval representing the expected network delay time. From Claim 52 limitation,  $\delta$  represents a minimum freshness restraint pertaining to the particular assertion. The freshness restraint refers to a time limitation and can be taken to mean  $\Delta t_1 + \Delta t_2$  because they both represent an interval of time that represents some form of restriction on time.

6. With respect to Claim 53, Abadi on page 202, 2<sup>nd</sup> paragraph, 5<sup>th</sup> sentence says that timestamps are used to prove that messages are fresh and the server's message that contains encryption keys do contain a timestamp as well (see Abadi, Fig. 1). The timestamped message contains a key that once received by A is used to decrypt the message. Hence, if A is able to decrypt this message, it has verified that the message comes from S. This is the validity assertion that the attorney fails to recognize.

7. The second limitation of Claim 53 of "means for asserting freshness constraints indicating a length of time and the initial assertions that the freshness constraints relate to" is met by Abadi on page 204, column 1, lines 1-21. If a rule exists that implements a process for asserting freshness constraints, this makes the existence of means to execute this process as obvious. Furthermore, the cited disclosure shows timestamp/freshness verification occurs from the fact that the freshness of X is being proven by including a nonce i.e. a timestamp in the message X. Hence this reads on the applicant's limitation.

8. With respect to Claim 54, the limitation of the preamble of "protecting an authority of a distinguished principal and enforcing revocation when the authority is compromised is inherent on page 201, column 1 and 2. The authentication role plays a role of securing the systems (see Abadi, page 201, column 1). Authentication is accomplished through the use of encryption keys and timestamps. Hence, these resources allow the authentication system to protect the authority

Art Unit: 2135

of a distinguished principal (person, computer or server) in a computer system (see column 1 and 2 of page 201). Therefore, these three means are obvious from Abadi's disclosure.

9. With respect to Claim 55, Van Oorschot et al teaches the first four limitations on column 1, lines 30-67 and column 2, lines 1-9. The certification authority (CA) represents the delegating authority while freshness constraints are represented by the validity period. The validity period in a certificate implies a default expiry date of the certificate after which the certificate is invalid. This works the same exact way as a timestamp, whereby if the time is expired, it is no longer valid. The fourth limitation of Claim 55 has already been discussed above.

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 52-54 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Abadi et al in view of Denning et al.

With respect to Claim 52,

Abadi et al teaches:

Art Unit: 2135

“deriving freshness constraints from initial policy assumptions and an authentic statement” (see page 201, column 2, including Fig. 1).

“imposing freshness constraints by employing recent-secure authenticating principals to effect revocation” (see page 201, column 2, including Fig. 1).

Abadi et al however does not explicitly teach the expression of  $|t_{\text{now}} - t_{\text{timestamp}}| < \delta$ . Denning however shows this.

Denning et al teaches “verifying that a relation  $|t_{\text{now}} - t_{\text{timestamp}}| < \delta$  is satisfied for verification of a secure channel, where  $t_{\text{timestamp}}$  being a time of a time stamp pertaining to a validity assertion of a particular assertion,  $\delta$  being a minimum necessary freshness constraint pertaining to the particular assertion and  $t_{\text{now}}$  being the time of verification” (see page 534, column 2, lines 1-16).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Denning et al within the system of Abadi et al because as Denning et al states in the cited section, this protocol protects against replay attacks.

Therefore, it would have been obvious to employ the teachings of Denning et al within the system of Abadi et al to obtain the claimed invention.

With respect to Claim 53,

Abadi et al teaches:

Art Unit: 2135

“means for creating a time stamped validity assertion message pertaining to the validity of an initial assertion” on page 202, second paragraph, 5<sup>th</sup> sentence.

“means for asserting freshness constraints indicating a length of time and relating to said initial assertion” on page 204, lines 1-21, column 1.

Abadi et al however does not explicitly teach the expression of  $|t_{\text{now}} - t_{\text{timestamp}}| < \delta$ . Denning however shows this.

Denning et al teaches “means for verifying that a relation  $|t_{\text{now}} - t_{\text{timestamp}}| < \delta$  is satisfied where  $t_{\text{timestamp}}$  is a time stamp contained in said message,  $\delta$  is a selected constant that represents a minimum necessary freshness constraint pertaining to said initial assertion and  $t_{\text{now}}$  is the time of verification” on page 534, column 2, lines 1-16.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Denning et al within the system of Abadi et al because as Denning et al states in the cited section, this protocol protects against replay attacks.

Therefore, it would have been obvious to employ the teachings of Denning et al within the system of Abadi et al to obtain the claimed invention.

With respect to Claim 54,

Abadi et al teaches:



Art Unit: 2135

“a first means for issuing an authoritative assertion by a distinguished principal; a second means for asserting freshness constraints on the assertion; a third means for asserting a time stamped validity assertion to the assertion indicating the validity of the assertion at the time of the time stamp” on page 201, column 2.

Abadi et al however does not explicitly teach the expression of  $|t_{\text{now}} - t_{\text{timestamp}}| < \delta$ . Denning however shows this.

Denning et al teaches “means for verifying that a relation  $|t_{\text{now}} - t_{\text{timestamp}}| < \delta$  is satisfied for each particular assertion necessary for verification of a secure channel, where  $t_{\text{timestamp}}$  being the time of a time stamp pertaining to the validity assertion of the particular assertion,  $\delta$  being the minimum necessary freshness constraint pertaining to the particular assertion, and  $t_{\text{now}}$  being the time of verification” on page 534, column 2, lines 1-16.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Denning et al within the system of Abadi et al because as Denning et al states in the cited section, this protocol protects against replay attacks.

Therefore, it would have been obvious to employ the teachings of Denning et al within the system of Abadi et al to obtain the claimed invention.

With respect to Claim 56, the limitation “means for preparing a statement of an assigned revocation authority in a distributed system network in response to a policy, said revocation authority statement being associated with an initial statement” is met on page 204, columns 1 and 2; “means for preparing a statement of a freshness constraint period in the distributed system network in response to said policy, said freshness statement being associated with said revocation authority statement” is met on page 204, columns 1 and 2 and section 2.3 on page 205; “means for preparing a validity statement at said assigned revocation authority in the distributed system network in response to said policy, said validity statement including a verification status at some temporal reference” is met on page 204, columns 1 and 2 and section 2.3 on page 205; “means for providing said revocation authority statement, said freshness statement, and said validity statement to a verification authority in the distributed system network” is met on page 204 and 205; and “means for selectively verifying said initial statement at said verification authority in response to said initial statement, said revocation authority statement, said freshness statement, and said validity statement” is met on page 204, columns 1 and 2, page 205, section 2.3.

Claim 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot et al (5699431) in view of Denning et al.

Van Oorschot et al teaches:

“means for issuing certificates for principals within an organization by the organization; means for asserting, by the organization, a principal authorized as an

Art Unit: 2135

authority for issuing time stamped certificates; means for delegating authority for issuing time stamped certificates; means for asserting freshness constraints on assertions” on column 1, lines 30-67 and column 2, lines 1-9.

Van Oorschot et al however does not explicitly teach the expression of  $|t_{\text{now}} - t_{\text{timestamp}}| < \delta$ .

Denning however shows this.

Denning et al teaches “means for verifying that a relation  $|t_{\text{now}} - t_{\text{timestamp}}| < \delta$  is satisfied for each particular assertion necessary for verification of a secure channel, where  $t_{\text{timestamp}}$  being a time of a time stamp pertaining to the validity assertion of a particular assertion,  $\delta$  being a minimum necessary freshness constraint pertaining to the particular assertion and  $t_{\text{now}}$  being the time of verification” on page 534, column 2, lines 1-16.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Denning et al within the system of Van Oorschot et al because as Denning et al states in the cited section, this protocol protects against replay attacks.

Therefore, it would have been obvious to employ the teachings of Denning et al within the system of Van Oorschot et al to obtain the claimed invention.

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

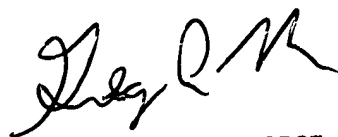
A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tracey Akpati whose telephone number is 703-305-7820. The examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

OTA



GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100